(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2002 (03.01.2002)

PCT

(10) International Publication Number
WO 02/01381 A1

(51) International Patent Classification[7]: G06F 15/173, 15/16

(21) International Application Number: PCT/US01/19642

(22) International Filing Date: 19 June 2001 (19.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/605,124 28 June 2000 (28.06.2000) US

(71) Applicant and
(72) Inventor: BUNCH, Clinton, D. [US/US]; 214 Spinner Road, DeSoto, TX 75115 (US).

(74) Agent: GRIGGS, Dennis, T.; Suite 1000, 17950 Preston Road, Dallas, TX 75252 (US).

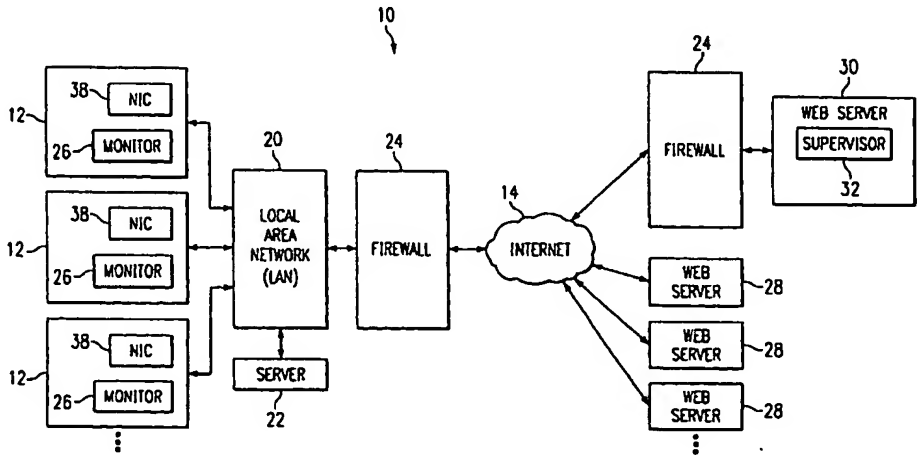
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR TRACKING TIME SPENT AND DESTINATIONS OF CLIENT COMPUTERS CONNECTED TO THE INTERNET



(57) Abstract: Employee Internet usage is monitored to identify the web sites employees visit and the amount of time employees spend at each site. The monitoring system (10) utilizes a client-based module (26) that monitors Internet access and operates in conjunction with an enforcement supervisor module (32) located on a remote web server (30). The client-based module (26) performs all of the monitoring and logging activity. A log containing the web page title, location (URL) and time spent is stored by the client-based monitoring module (26) in memory (48) on the client computer (12). The web page title and URL are obtained from system notifications from the browser (36) to the client component. The client computer (12) uploads the log containing the web page information to the web-based supervisor module (32).

WO 02/01381 A1

Description

SYSTEM AND METHOD FOR TRACKING TIME SPENT AND DESTINATIONS OF CLIENT COMPUTERS CONNECTED TO THE INTERNET

Technical Field

The present invention relates generally to information processing, and in particular to systems and methods for monitoring access and usage of individual computer systems and local area networks connected to larger open networks (wide area networks), including the Internet.

Background Art

The explosive growth of the Internet, particularly the World Wide Web, has had a dramatic effect on the way many corporations and other organizations do business. The Internet brings a world of information to the fingertips of employees.

However, some of what the Web introduces into the workplace can be non-productive and damaging to a business. Employees who waste company time or resources on non-work-related activities can become a drain on the company. If Internet bandwidth is used for downloading pornography or making personal travel reservations, it could mean slower access for employees doing work. Fellow employees could be exposed to inappropriate material that could ultimately lead to a sexual harassment lawsuit. Just as it is inappropriate to pass around certain materials at work, it is inappropriate for employees to be viewing certain material on company computers, especially if other employees may be unwittingly exposed to that material.

As a result, corporate information system departments face new challenges. Companies are increasingly looking for the best way to manage Internet access, and keep objectionable online material out of the workplace. One hundred twenty-two million employees are expected to access the Internet, and 660,000 companies are

expected to implement Internet productivity systems in the year 2000.

One extreme solution is to build a company-wide intranet. However, the company's knowledge-base may not include the information an employee needs. Also, as the use of E-mail becomes more accepted and the Internet continues to grow, cutting employees off from the Web does not make good business sense.

The software industry has introduced a number of products and technologies that are designed primarily to monitor and track the web sites visited by users. Most, if not all of these products are based on filtering software.

Filtering software is designed to help companies control recreational and personal Internet use. The software monitors employee use of the Net and, depending on how it is configured by the employer, prevents employees from visiting certain types of Web sites that could interfere with productivity, tie up Internet bandwidth or violate company policies.

Some filtering software contains what the company calls its list of sites that are inappropriate for employees. Blocked sites are divided into categories so that companies can enable access to specific content categories according to the time of day. For example, an employer could permit access to entertainment sites during the lunch hour or after hours.

To that end, software can be used to deny employees access to sites in such areas as astrology and mysticism, games, entertainment, travel, news, job searches, investment, hobbies and more. In other words, anything an employee might want to do that's not directly related to his job.

Access levels can be defined on the basis of time of day or the day of the week. The employer could, for example, give users access to a wider range of web sites after 6 p.m. or on weekends. The employer could

also define different levels of Internet access for different individuals or groups in the company.

A human resource department, for example, could have access to job search Web sites that might be off-limits to other employees. The chief executive could have unlimited access and still restrict what others can do.

Filtering software is not without limitations. Much of the software won't run on systems with a modem connection to the Internet. The filtering software requires a server-based mechanism such as a Microsoft or Netscape proxy server or a check point firewall.

While the server-based mechanisms have the advantage of not requiring software to be installed on the client machine, they are incapable of monitoring the actual time spent by the user on any given web page. In addition, LAN server-based mechanisms have the disadvantage of imposing significant performance penalties, especially if the number of clients connected to it is large. This approach usually requires technical expertise since it is difficult to administer and configure.

Filtering software does a good job of blocking out the offensive sites, but the software may inadvertently restrict information that the employee may need. For example, an employee researching breast cancer, or an HR director putting together a presentation on the topic of sexual harassment in the workplace may not be able to obtain the relevant information. Additionally, filtering software requires constant updating due to new web sites with offensive content going on-line daily.

Also, a moderate amount of employee use of the Internet for personal business isn't necessarily counterproductive. Just as most employers tolerate a certain amount of personal phone calls at work, it may be perfectly acceptable for an employee to use a company PC to make personal travel arrangements, book a dinner

reservation, check a stock portfolio or read the newspaper during personal break time.

Another software industry solution, client-based filters (e.g. Surfwatch and CyberPatrol) that prevent users from accessing undesirable Web sites, do not adequately overcome the limitations of centralized filtering. Designed largely as parental control tools for individualized PCs, these programs are easily disabled by uninstalling (accidently or intentionally) the filter. For example, a Windows user can simply reinstall the Windows OS, replacing certain driver files of the filter. This disables the filter and provides the user with unrestricted access to the Internet.

A solution has not yet been proposed to deal with the problems posed by Internet access in the corporate environment. There is a need for a simple system and methods providing companies the means to monitor the exchanges permissible between a local computer and an external network or WANs, including the Internet.

Disclosure of the Invention

Perhaps the two aspects of Internet access most important to the productivity of an organization are 1) the ability to monitor the amount of time employees spend on the Internet and 2) the web sites employees visit while on the Internet. Although the Internet is an increasingly important business tool, it also poses a temptation for abuse. Employees may be tempted to pursue their own private interests while on the job. The Internet access monitoring system of the present invention addresses this problem by allowing an organization to monitor employee Internet access on a time-spent-per-page and total time-per-week basis. The actual monitoring can be done in a variety of ways, including monitoring the time and web site history of an employee actively interacting with the Internet, and/or monitoring the complete time and web site

history of particular groups of users accessing the Internet.

The present invention addresses the bandwidth concerns by limiting access to the Internet to certain times of the day and monitoring employees. When an employee knows that he is being monitored, he is much less likely to surf inappropriate material on the Internet.

The present invention provides system and methods for client-based monitoring of Internet access, which operate in conjunction with an enforcement supervisor located on a remote web server. In accordance with the present invention, a central filter and centralized enforcement supervisor are not used. Instead, the present invention provides a client side mechanism for tracking Internet usage on a time-spent-per-web-page basis within a browser such as Microsoft Internet Explorer and transmitting this information to a remote web site (over the Internet or any other network) where authorized personnel can access the information over the Internet.

The client-based monitoring module in a preferred embodiment performs all the monitoring and logging work. Each time the user navigates to a new web page, the previous web page title, location (Universal Resource Locator or URL), and time spent are then stored by the client component in memory on the client computer. The web page title and URL are obtained from system notifications from the browser to the client component. The client computer uploads the log containing the web page information to a web-based supervising module.

The present invention provides guidelines that can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month or the like), and the time a user can interactively use the Internet (e.g., per day, week, month, or the like). These guidelines can be qualified by optionally specifying: to whom should a rule apply (list of users, list of work

groups, or all); time of day when the rule should be applied (for example from 9 a.m. to 5 p.m.).

All the logged information is viewable by an administrator in either a summary format (total number of hours spent by each user) or in a detailed format (time per web page with details such as the web page tile, URL, and time) by visiting the web site and entering the Administrator authentication information. This function is the same as that of a history log except that a web-based format does not permit modification by the client machine.

Brief Description of the Drawing

Various advantages and features of the invention will be understood from the following detailed description taken in connection with the appended claims and the attached drawing figures in which:

FIGURE 1 is a block diagram providing an overview of a Internet-based (client/server) system in which the present invention is embodied;

FIGURE 2 is a block diagram providing an overview of a Internet-based (client/server) system in which the present invention may be embodied;

FIGURE 3 is a block diagram illustrating a client-side monitor;

FIGURE 4 is a block diagram illustrating a web-side supervisor server;

FIGURE 5 is a flow chart illustrating a method of the present invention for handling a user session;

FIGURE 6 is a flow chart illustrating a method of the present invention for handling the acquisition of the Internet monitoring system; and

FIGURE 7 is a bit map screen shot illustrating a preferred user interface or wizard dialog for configuring first-time user registration.

Best Mode for Carrying out the Invention

The present invention provides system and methods for client-based monitoring which operate in conjunction with a web-based enforcement supervisor. In accordance with the present invention, a central filter and centralized enforcement supervisor are not used. Instead, the present invention provides a client side mechanism for tracking Internet usage on a time-spent-per-web-page basis within an Internet browser such as Microsoft Internet Explorer and transmitting this information to a remote web site (over the Internet or any other network) so that it is easily accessed by authorized personnel over the Internet.

An Internet access monitoring system, constructed in accordance with the present invention, preferably supports the maintenance of a detailed log of Internet access, for enforcing the guidelines. An Internet access monitoring system, constructed in accordance with the present invention, preferably supports guidelines. The present invention provides guidelines that can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month or the like), and the time a user can interactively use the Internet (e.g., per day, week, month, or the like). These guidelines can be qualified by optionally specifying: to whom should a rule apply (list of users, list of work groups, or all), and time of day when the rule should be applied (for example from 9 a.m. to 5 p.m.).

All the logged information is viewable by an administrator in either a summary format (total number of hours spent by each user) or in a detailed format (time per web page with details like the web page tile, URL, and time) by visiting the web site and entering the Administrator authentication information. This function is the same as that of a history log except that a web-based format does not permit modification by the client machine.

The present invention addresses the bandwidth concerns by limiting access to the Internet to certain times of the day and monitoring employees. When an employee knows that he is being monitored, he is much less likely to surf inappropriate material on the Internet.

The system hardware of the client-side Internet access monitoring module and server-based Internet access supervisor employed in a preferred embodiment, will now be described in further detail.

Referring to FIGURE 1 and FIGURE 2, the invention is generally embodied on a computer system 10 including one or more personal computer systems, such as a desk-top personal computer 12. Preferably the personal computer system is an IBM PC-compatible personal computer, available from a variety of vendors (including IBM of Armonk, NY and Compaq Computer Corporation of Houston, TX), but the personal computer system 12 could be a wireless telephone with Internet capability or the like. In the alternative, with the growth of remote computerized appliances, the present invention is useful to control television viewing, computer game usage, cell phone usage and the like.

Referring to FIGURE 1, the personal computer system 12 is connected to a wide area network 14 by a modem 16. In the preferred embodiment, the WAN is the Internet or World Wide Web. Preferably, the modem 16 provides SDSL or ADSL service (e.g., available from Jump.net of Austin, TX), but the modem could be a conventional 56K modem (e.g., available from U.S. Robotics), ISDN line or the like.

Referring to FIGURE 2, in an alterative embodiment, the personal computer system 12 is connected to the WAN 14 by a network interface card 18 and a local area network 20 which has a server 22 and a firewall 24.

Referring to FIGURE 1 and FIGURE 2, the personal computer system 12 includes a client-side Internet access monitoring module 26 of the present invention.

The Internet allows access to a multitude of web servers 28. Of particular interest is a supervisor web server 30 which includes a web-side Internet access monitoring supervisor module 32 of the present invention and a firewall 24. In an alternative embodiment, the web-side Internet access monitoring supervisor module 32 is located on the server 22.

The web site Internet access monitoring supervisor module 32 and client-side Internet access monitoring module or client module 26 prevent users from circumventing Internet monitoring, either accidentally or intentionally. It should be difficult, for instance, for a user to circumvent Internet monitoring by connecting to the Internet through a dial-up connection (e.g., connecting to an ISP with a modem). The monitoring system of the present invention is triggered by the Internet browser, not the Internet connection, making circumvention difficult. Similarly, it should be difficult for a user to circumvent access rules by installing, uninstalling or tampering with components of his own PC or the monitoring system. The minimum number and small size of client-side components of the present invention makes tampering difficult and software conflicts unlikely. Each personal computer system has one client-side module that is less than one megabyte in size.

Construction and operation of the client-side Internet access monitoring module, including its interaction with server-based components employed in a preferred embodiment, will now be described in further detail.

A user session with respect to the client-side monitoring module will now be described in further detail. Referring to Figure 3, the personal computer system 12 includes the client-side monitoring module 26, an operating system (OS) 34, and an Internet browser 36. The client-based monitoring module 26, which in a preferred embodiment performs all the monitoring and logging work,

is responsible for intercepting universal resource link requests between an Internet browser and a network programming interface.

The operating system has the network programming interface component 38 for communications between the Internet browser 36 and the WAN or Internet 14. Preferably, the operating system (OS) is Microsoft Windows 95, 98, 2000, or NT (available from Microsoft Corporation of Redmond, Washington), but the OS 34 could be Linux, Apple OS/9 or another operating system. Microsoft's Windows operating system has a network programming interface component 38 known as Windows sockets for use by application software to communicate on the Internet. The Windows sockets is implemented in the Windows operating system as a dynamic link library named WSOCK32.DLL. A prior version for 16-bit software is implemented in a file named WINSOCK.DLL.

An Internet browser 36 which utilizes the network programming interface 38 for communicating on the Internet generally does not control the computer's connection to the Internet 14, but rather simply calls the Windows sockets to communicate over the Internet 14. Preferably, the Internet browser 36 is Internet Explorer (available from Microsoft Corporation of Redmond, Washington), but the Internet browser could be some other browser such as Netscape Navigator.

Internet Explorer allows certain of its function calls to the network programming interface 38 to be monitored by the software module, including the client-side module, with a hook interface 40. The hook interface 40 is a function exported by the client-based software or other monitoring software module for monitoring requests from Internet Explorer to the network programming interfaces 38. In the computer software field, the term hook generally refers to the ability for one application to monitor or receive notification about function calls made by another application to yet a third application, a

system component, or an application programming interface. A hook interface is a mechanism by which an application registers to receive notification information from a hook.

The client module 26 is programmed to intercept events from Internet Explorer browser 36 by following these steps:

1. Registering itself in the Windows Registry to be loaded upon browser startup;

2. Implementing the IObjectWithSite interface published by Microsoft; and

3. Implementing the IObjectWithSite::SetSite() method. This method allows the application to request a pointer to Internet Explorer's IWebBrowserEvents2 Interface. This interface may be used to intercept events from Internet Explorer.

The following Microsoft links have further technical details, which are incorporated herein by reference:

http://support.microsoft.com/support/kb/articles/Q179/2/30.ASP;

http://msdn.microsoft.com/workshop/browser/webbrowser/reference/IFaces/DWebBrowserEvents2/DWebBrowserEvents2.asp; and

http://support.microsoft.com/support/kb/articles/Q179/2/30.ASP.

Alternatively, the open source version of the Netscape Navigator browser (e.g., available from www.mozilla.org) can be configured to allow certain of its function calls to the network programming interface 38 to be monitored by a software module, such as the client-side module 26, with the hook interface 40.

Whenever the hook interface 40 hooks a URL request to the network programming interface 38, the hook interface determines that the Internet browser 36 is attempting to communicate over the Internet 14. The hook interface 40 sends the URL request to the client-based

monitor and sends the URL request to the network programming interface 38.

A user might attempt to circumvent the system by loading an authorized browser. This invention has the ability to perform a periodic search of the files on the personal computer system or client computer 12 to determine file names associated with other browsers. This is accomplished by comparing a compiled list of file names associated with unauthorized browsers. Violations are reported to a designated administrator via email.

The client-based monitor contains a user authentication application 42, a timer 44, an user display application 46, and a temporary history log cache 48. The user authentication module 42 presents the user with a log-in prompt, accepts the user's name and password and forwards this information to the web-based server.

The timer application 44 synchronizes its internal time to the server time. The current time is maintained by the client component 26 independently of the computer system time in order to prevent users from subverting the system by changing the time clock in the OS 34.

The timer application processes (i) the number of permitted minutes/week, (ii) the number of minutes already consumed this week, (iii) the monitored and restricted start and end times, and (iv) the current system time at the web-based server 30.

Also, the timer application 44 processes the URL requests from the hook interface 40. The timer application 44 logs all the URL requests in the temporary history log cache 48 on a time-spent per page basis. By logging all the times that URL requests are made, the system can create a comprehensive representation of a user's Internet activities.

The timer 44 of the client module 26 is programmed to record time-spent-per-URL by following these steps:

1. Implementing the DwebBrowserEvents2: :Navigate-Complete2 method to be notified each time a new URL is navigated to;

2. Each time a new notification is received, the URL is stored in memory along with the current time at which it is received. The time spent on the previous URL is the difference between the current time and the time stored corresponding to the previous URL; and

3. The temporary history log cache 48 will contain the sequence of URL, begin time and time spent records in memory on the client module 26.

If the user exceeds permitted time during the monitored period, the client component 26 will notify the user and request that the user terminate the browser 36. If the user fails to terminate the browser 36, then a violation will be reported to the web server 30 and an email notification will be sent to a supervisor. Likewise, if the current time period changes from monitored to restricted, then the user is notified.

The user display application 46 provides a periodically updated visual display to the user. This display includes the amount of authorized time a user has remaining on the Internet and the period of use (restricted/unrestricted). The timer 44 considers the time the browser 36 is minimized to be inactive time. The client-based module 26 knows when the browser 36 is minimized by utilizing the following methodology: upon startup a reference (or handle) to the main browser window is obtained and stored in memory by the client module. At regular intervals this reference handle is queried for its current state (by using the "IsIconic()" OS API) in order to determine if the window has been minimized or not. In an alternative embodiment, the time-keeping function of

this invention allows for calender functions, including on-the-job timekeeping for remote employee users.

The temporary log cache 48 stores the time stamped URL requests sent from the timer application. Also, the temporary log cache 48 stores the gateway web site. The gateway web site is the web site the user is directed to after authentication. The gateway web site can either be determined by the subscriber (employer) or through commercial arrangements with various companies interested in becoming a point of entry for users. This can be established by creating a brief user profile upon user registration. The user can then be introduced to a number of sites which are of particular interest to their profession or group. This entry point is similar to the home page concept, with the exception that it cannot be changed by the user.

Referring to FIGURE 5, a user begins an Internet session by opening his Internet browser. The browser helper object model offered by Internet Explorer allows the client component to load up whenever the browser starts. At step 50, a user authentication module presents the user with a log-in prompt. The user is asked to enter his user name and password.

At step 52, the Internet browser 36 automatically connects to the supervisor web site 30. At step 54, the client component transmits the authentication information for verification to the web site using the same protocol used by the browser (i.e., an HTTP or HTTPS POST operation). The web site server 32 indicates success or failure.

In the case of authentication failure, the user is permitted to either retry, exit the browser 36 or ignore the authentication in which case the client component 26 notifies the web site server 30 of the violation. The web site server 30 saves this information in the database and may send out an e-mail to the

administrator. The present invention allows for continued Internet access even in the event of a server failure.

In the case of authentication success case, the web server 30 returns the following information and guidelines: (i) number of permitted minutes/week; (ii) number of minutes already consumed this week; (iii) the monitored and restricted start and end times; and (iv) the current system time at the server. In the preferred embodiment, the server returns a gateway web site.

The user display application of the client component notifies the user about the remaining time as well as the current period (Monitored, Restricted or Unrestricted) and then starts a visible timer on the client machine. This timer is used to track the time spent on every web page visited by the user.

At step 56, the user is presented with a gateway web site. At step 58, a user Internet session begins. The user may go to any URL. Each time the user navigates to a new web page, the previous web page title, location (Universal Resource Locator or URL), and time spent are then stored by the client component 26 in memory on the client computer. The web page title and URL are obtained from system notifications from the browser to the client component 26.

Periodically, at step 60, the client monitoring module 26 reconnects to the server web site. Upon reaching preset limits (such as number of records, time elapsed, etc.) or on termination of the browser process, the client component 26 will transmit this cached information to the web site server 30. The latter will store this information in a database under the appropriate user's history log.

At step 62, the user ends the Internet session by closing his web browser. At step 64, the client monitoring module 26 connects to the supervisor web site 30. The supervisor web site authenticates the log-in

information and the client monitoring module 26 uploads the temporary history log cache. The user Internet session is completed.

If the user exceeds his permitted time during the monitored period, then the client component 26 will notify the user and request that the browser 36 be terminated. If the user fails to do so, then the violation is reported as before. Likewise, if the current time period changes from Monitored to Restricted, then again the user is notified as before.

The operation of the web-based supervisor module will not be described in detail. The system allows administrators and users to log-in to the web-based supervisor server and read reports on Internet usage. The reports of the supervisors are much more detailed. Referring to FIGURE 4, the web-based supervisor 30 includes an administrative web pages application 68, a client communication interface 70, a permanent history log 72, an authentication service and configuration information storage application 74, and an email notification service application 76.

The administrative web pages application 68 processes and presents all web-page requests which the server receives. The client communication interface 70 receives and processes requests from the client-based module 70.

The permanent history log records the information from the client-based temporary history cache 48. This information is viewable by an administrator in either a summary format (total number of hours spent by each user) or in a detailed format (time per web page with details like the web page tile, URL, and time) by visiting the web site and entering the Administrator authentication information. This function is the same as that of a history log of Internet Explorer, Netscape Navigator, or Netscape Communicator except that a web-based format does not permit modification by the client machine.

The supervisor web site authenticates the log-in information and the client monitoring module uploads the temporary history log cache 48 to the server web site 30. The client communication interface accepts the temporary history log cache and sends it to a permanent history log 72.

Referring to FIGURE 6, a company representative acquires the Internet monitoring system. At step 74, the company representative visits the server web site and decides to register his company for the Internet monitoring system. At step 76, the company representative clicks on the first time user registration hyperlink. At step 78, the company representative answers questions about his company. These questions include company name, address, and the like. Referring to Figure 7, a First-Time User Registration interface is shown.

Referring again to Figure 6, at step 80, the company representative decides how many licenses to purchase. At step 82, the company representative sets up the company hierarchy. In order to effectively manage Internet access, a system should support existing organizational structures. A department supervisor, for example, should be able to determine the needs of his subordinates within a safe overall framework. This is important for the overall success of Internet access within the organization as it allows supervisors to address any problems which arise early on (before they become serious personnel issues).

Accordingly, the Internet access monitoring system of the present invention supports a hierarchical structure where individual supervisors can monitor and set the access rules for their individual workgroups without affecting others in the organization. At the same time, a central authority (e.g., corporate IS department) still can establish general rules that cannot be overwritten on the workgroup level.

The company representative proceeds to configure groups of users. Each group may be assigned times during the day when users belonging to that group may be restricted from accessing the Internet and other times during which they may be permitted monitored access to the Internet. During a monitored period, all Internet access is logged and timed. Other times of the day are considered to be unrestricted periods during which Internet access is not monitored.

The company representative then proceeds to set up individual users belonging to these groups by inputting names, e-mail addresses and authentication information for each user.

At step 84, the web site sends an e-mail to each new user with information about downloading and installing the client-side software component required for client-based monitoring.

Industrial Applicability

The following examples demonstrate typical applications of this system. Consider, for instance, employee Ralph who begins routinely accessing pornographic sites on the Internet during business hours. Ralph's activities are prohibited by company policy, and are taking up vital bandwidth. Using current technology, the company's IS department would likely not detect the activity for weeks, or even months, as the department's main focus is to keep the company's networks running smoothly, not to track individual activities. At the point when the activity is uncovered, Ralph might have already violated company policy to the point where his manager has no choice but to dismiss Ralph. If Ralph's Internet access activity is monitored locally by Ralph's supervisor, however, the supervisor can notice the prohibited activity almost immediately. After reminding Ralph of company policy, the supervisor can continue to

monitor Ralph's on-line activities and head off the need to terminate Ralph.

As another example, consider Donna's company, a small company that cannot afford an expensive server and the technical expertise to support the server. Donna wants to monitor her employees' Internet access, but can not afford a conventional Internet monitoring system requiring a LAN server and technical expertise. However, Donna can afford the Internet access monitoring system of the present invention since it does not require a local server or technical expertise.

As another example, consider Tommy, an employee who normally has very little Internet access but needs to write a competitive analysis for a new product. To complete this task effectively, Tommy requires Internet access for performing required research. Conventionally, Tommy's supervisor would call the company's IS department to arrange the appropriate Internet access, a process requiring days or even weeks. However using the Internet access monitoring system of the present invention, Tommy accesses the Internet as required to finish his project and the Administrator does not act on the warning e-mail.

Claims

1. In a system comprising a plurality of personal computers having Internet access, a method for monitoring the Internet access for a particular personal computer, the method comprising:

providing at the particular personal computer a client-based monitor module;

providing at a web server a web-based supervisor module, said supervisor module specifying guidelines which govern Internet access by the personal computer;

sending guidelines from the supervisor module to the personal computer monitor module;

at the client-based monitor module, logging a request for Internet access in a log, and logging any violations of the guidelines in the log; and,

sending the log to the supervisor module where the following sub-steps are performed:

(1) copying the log into a web-based log;

(2) notifying a designated administrator of any violation.

2. The method of claim 1, wherein the personal computer monitor module includes an Internet browser for processing requests for a particular Universal Resource Locator (URL), including the step:

hooking the Internet browser requests for a particular Universal Resource Locator.

3. The method of claim 1, including the step:

installing in the personal computer a client-based monitoring program which executes in response to the Internet browser requesting a universal resource locator (URL).

4. In a system comprising at least one personal computer having Internet access, a method for controlling the bandwidth usage on the Internet for the at least one personal computer, the method comprising:

providing at each personal computer a client-based monitoring module;

providing at a web server a web-based supervisor module, said supervisor module including usage guidelines which govern Internet access by each personal computer;

sending usage guidelines from the supervisor module to the personal computer;

at the client-based monitoring module, logging a request for Internet access in a log, and logging any violations of the guidelines in the log; and,

sending the log to the supervisor module and copying the log into a web-based log.

5. The method of claim 4, wherein the personal computer includes an Internet browser for processing requests for a particular Universal Resource Locator (URL) and including the step of:

hooking the Internet browser requests for a Universal Resource Locator at the particular personal computer.

6. The method of claim 4, the client-based monitoring process includes:

installing at the particular personal computer a client-based monitoring program which executes any time the Internet browser requests a universal resource locator (URL).

7. In a system comprising a plurality of personal computers connected to a network and having Internet access, a method for monitoring the Internet

access for a particular personal computer, the method comprising:

providing at the particular personal computer system a client-based monitor module;

providing at a web server a web-based supervisor module, said supervisor module including a program specifying guidelines which govern Internet access by the personal computer;

sending guidelines for supervisor module to the personal computer;

at the client-based monitoring module, logging a request for Internet access in a log, and logging any violations of the guidelines in the log; and,

sending the log to the supervisor module where the following sub-steps are performed:

(1) copying the log into a web-based log;

(2) notifying a designated administrator of any violation.

8. The method of claim 7, wherein the particular personal computer includes an Internet browser for processing requests for a particular Universal Resource Locator (URL) and including the step:

providing at the particular personal computer system a process which hooks the Internet browser requests for a particular Universal Resource Locator.

9. The method of claim 7, wherein said step of providing at the particular personal computer system client-based monitoring process includes:

installing at the particular personal computer a client-based monitoring program which executes any time the Internet browser requests a universal resource locator (URL).

10. The method of claim 7, wherein the personal computer system includes a server computer connected to the network.

11. The method of claim 7, including at least one other personal computer system connected to the network.

12. In a system comprising a plurality of similar computer systems having Internet access, a method for monitoring Internet access for a particular personal computer, the method comprising:

storing at a web-based supervisor computer a list of guidelines for Internet access;

transmitting said list from the supervisor computer to the personal computer;

at the personal computer, hooking a request for Internet access from an Internet browser;

if the request for Internet access violates the guidelines, notifying the supervisor computer of the violation.

13. In a system comprising a plurality of computers connected to a network and having Internet access, a method for monitoring Internet access for a particular personal computer, the method comprising:

storing at a web-based supervisor computer a list of guidelines for Internet access;

transmitting said list from the supervisor computer to the personal computer;

at the personal computer, hooking a request for Internet access from an Internet browser;

if the request for Internet access violates the guidelines, notifying the supervisor computer of the violation.

14. A computer system for regulating Internet access by users of personal computers comprising:

a plurality of client computers which can connect to at least one open network, each client computer including a monitor module means;

said monitoring module creating a database containing a history log of Internet access;

a supervisor module provided at a computer which is in periodic communication with each client computer to be regulated, said supervisor module including a database containing a history log of Internet access; and,

means for transferring the history log of Internet access from the personal computer system to the supervisor module over the open network.

15. The system of claim 14, further comprising means for searching personal computer system for certain file names.

16. In a system comprising a plurality of personal computers connected to a network and having Internet access, a method for monitoring the Internet access for a particular personal computer, the method comprising:

providing at the particular personal computer a client-based monitor;

providing at another computer on the network a supervisor, said supervisor specifying guidelines which govern Internet access by the personal computer, and a client hierarchy;

sending guidelines from the supervisor to the personal computer;

at the client-based monitor, logging a request for Internet access in a log, and logging any violations of the guidelines in the log; and,

sending the log to the supervisor where the following sub-steps are performed:

(1) copying the log into a web-based log;

(2) notifying one or more clients in the client hierarchy of any violation.

17. The method of claim 16, wherein the particular personal computer includes an Internet browser for processing requests for a particular Universal Resource Locator (URL) and including the step:

hooking the Internet browser requests for a particular Universal Resource Locator at the particular personal computer monitor.

18. The method of claim 16, including the step:

installing at the particular personal computer system a client-based monitoring program which executes in response to the Internet browser requesting a universal resource locator (URL).

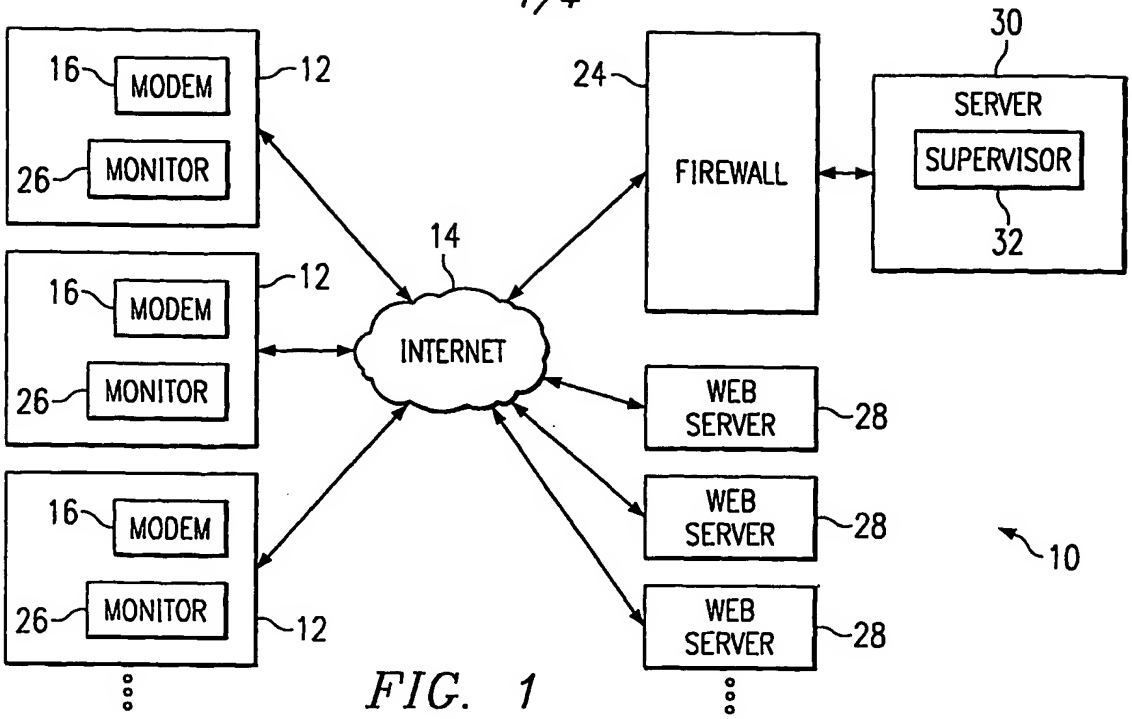

16
MODEM
12
26
MONITOR
16
MODEM
12
26
MONITOR
16
MODEM
26
MONITOR
12
14
INTERNET
24
FIREWALL
30
SERVER
SUPERVISOR
32
WEB SERVER
28
WEB SERVER
28
WEB SERVER
28
10

FIG. 1

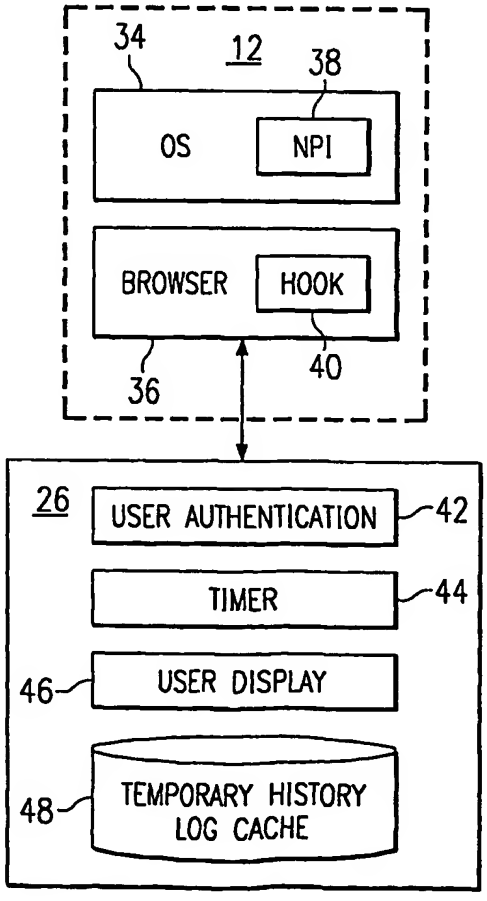

34
12
38
OS
NPI
BROWSER
HOOK
36
40
26
USER AUTHENTICATION
42
TIMER
44
46
USER DISPLAY
48
TEMPORARY HISTORY LOG CACHE

FIG. 3

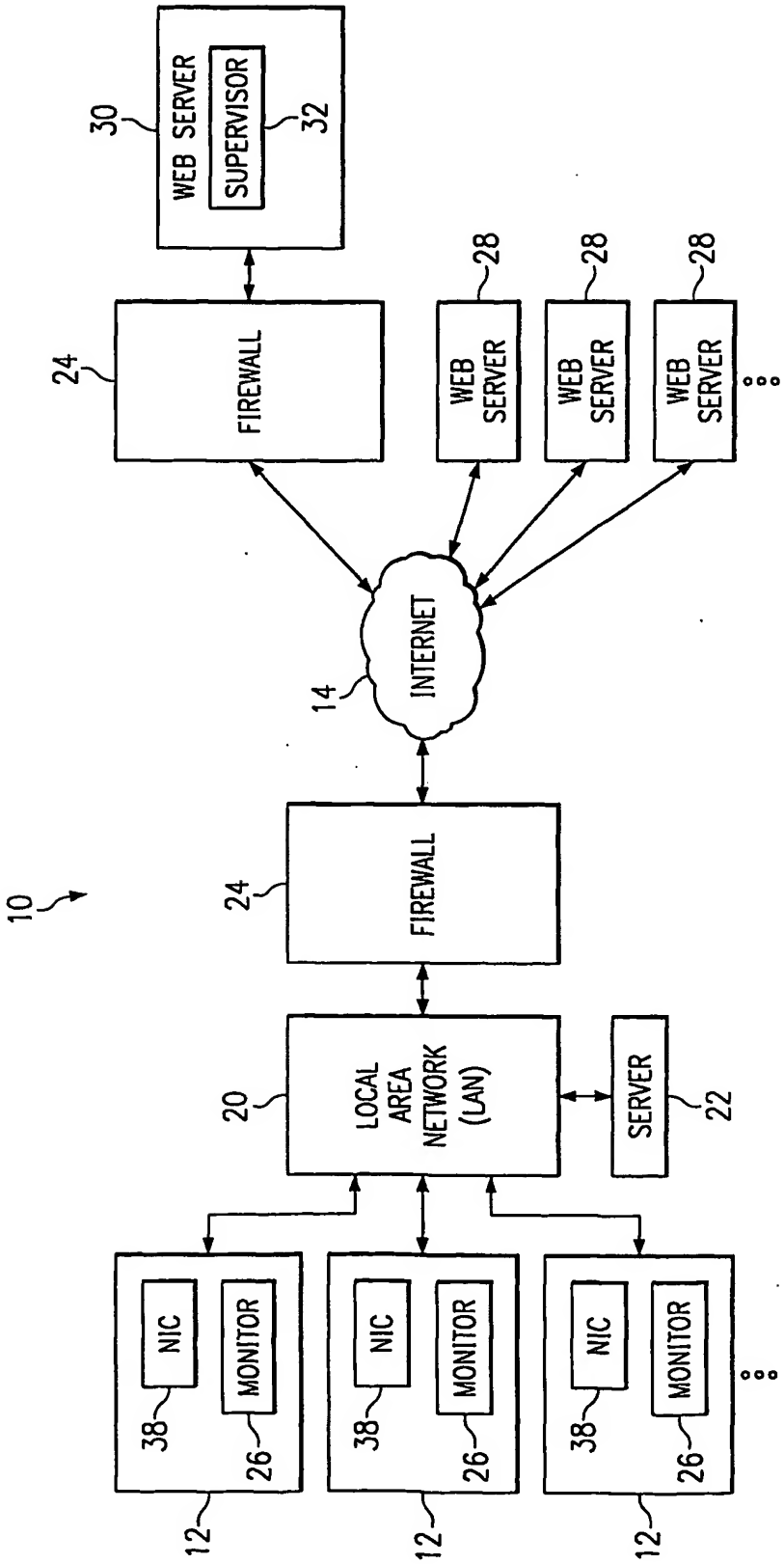

10
12
NIC
38
MONITOR
26
LOCAL AREA NETWORK (LAN)
20
SERVER
22
FIREWALL
24
INTERNET
14
WEB SERVER
28
WEB SERVER
30
SUPERVISOR
32

FIG. 2

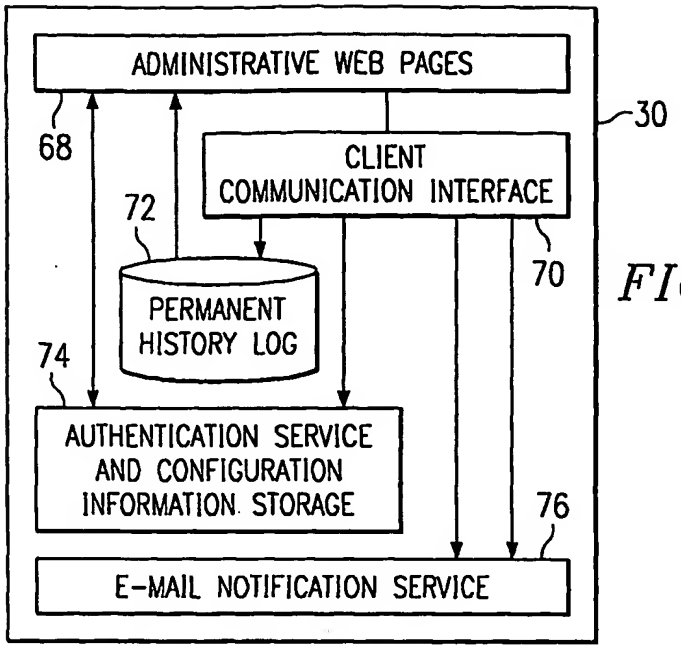


FIG. 4

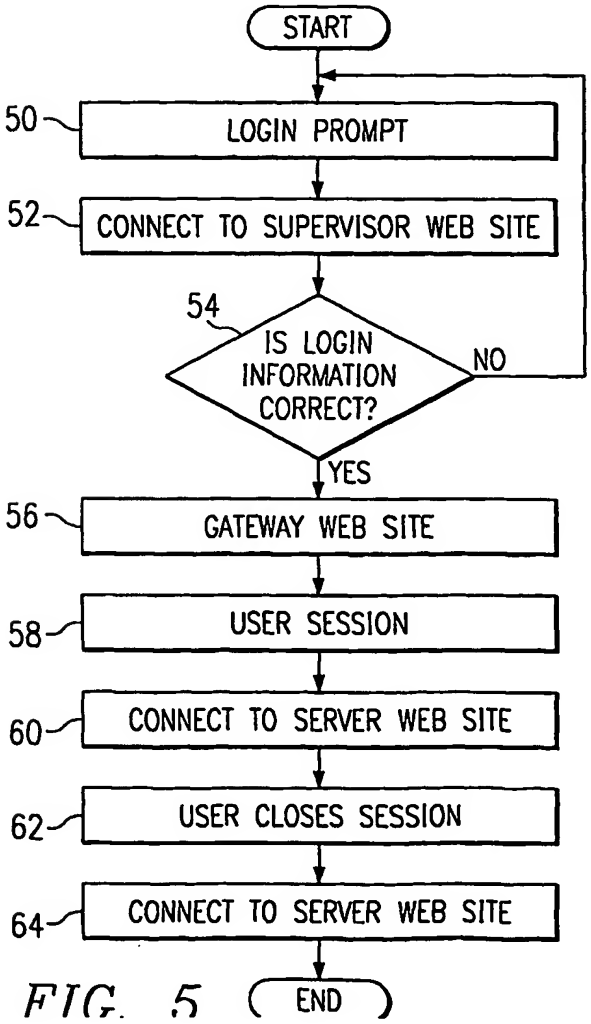


FIG. 5

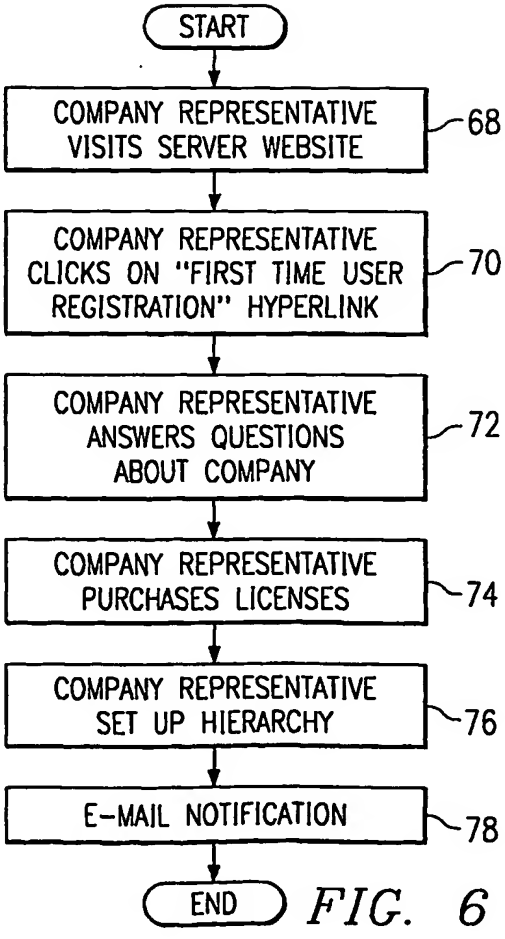


FIG. 6

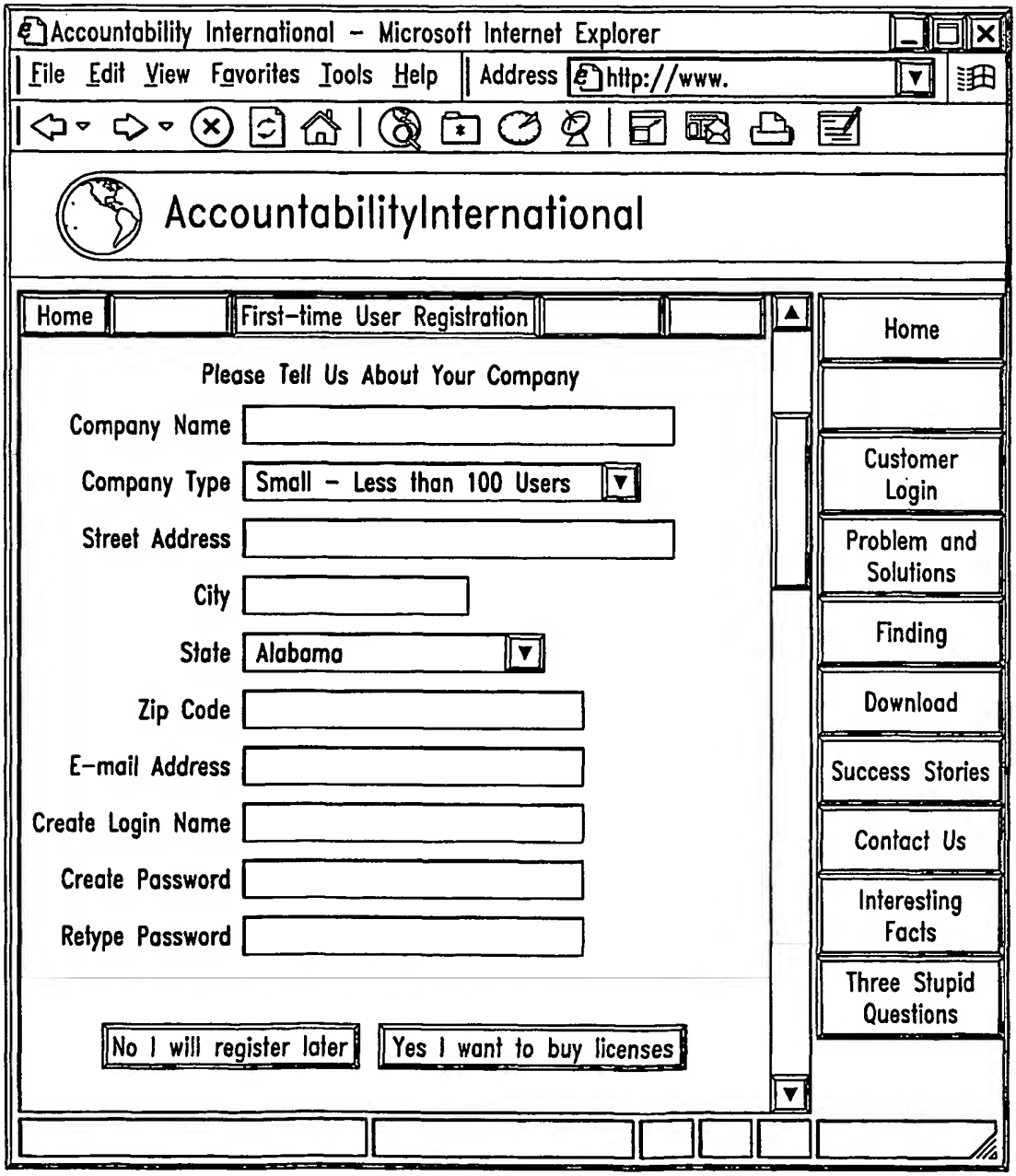

Accountability International - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.
AccountabilityInternational
Home
First-time User Registration
Please Tell Us About Your Company
Company Name
Company Type
Small - Less than 100 Users
Street Address
City
State
Alabama
Zip Code
E-mail Address
Create Login Name
Create Password
Retype Password
No I will register later
Yes I want to buy licenses
Home
Customer Login
Problem and Solutions
Finding
Download
Success Stories
Contact Us
Interesting Facts
Three Stupid Questions

FIG. 7

INTERNATIONAL SEARCH REPORT

Int[illegible]al application No.
PC[illegible]01/19642

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173, 15/16
US CL : 709/224, 203; 713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/224, 203; 713/200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN
search terms: log, list, record, violate, illegal, access, surfing, notify, alarm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 6,195,697 B1 (BOWMAN-AMUAH) 27 February 2001, col. 10, line 20 - col. 18, line 13 and col. 26, line 10 - col. 32, line 32.	1-18
A	US 4,672,572 A (ALSBERG) 09 June 1987, col. 2, line 9 - col. 3, line 25.	1-18
A	US 5,987,611 A (FRUEND) 16 November 1999, see entire document.	1-18
A	US 6,026,440 A (SHRADER et al.) 15 February 2000, col. 3, line 24 - col. 10, line 59.	1, 4, 7, 14, 16
A	US 6,070,190 A (REPS et al.) 30 May 2000, col. 5, lines 6 - col. 7, line 21 and col. 14, line 10 - col. 15, line 62.	1, 4, 7, 14, 16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 25 AUGUST 2001	Date of mailing of the international search report 26 SEP 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JASON D. CARDONE James R. Matthews Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet) (July 1998)*